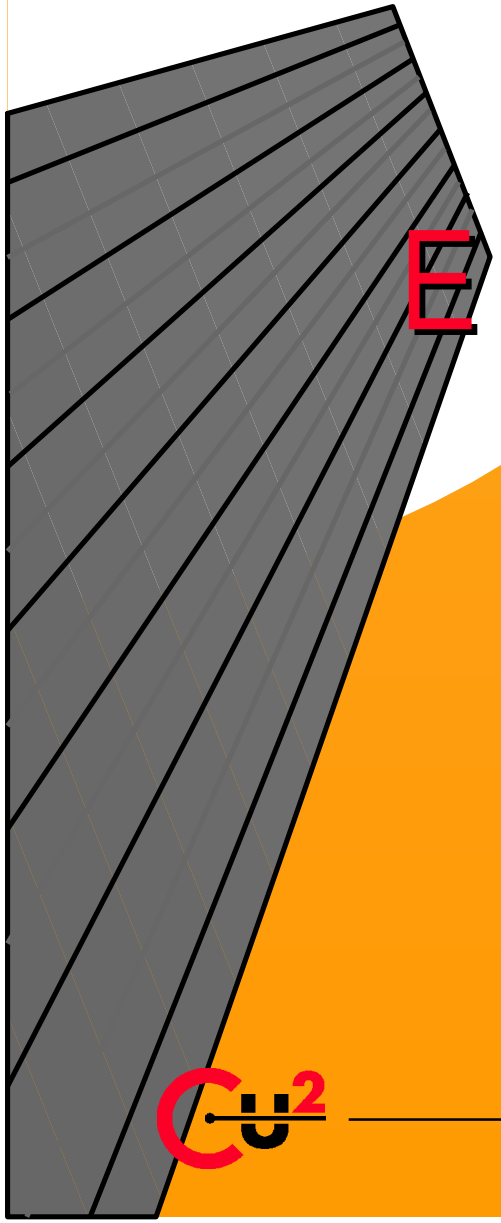
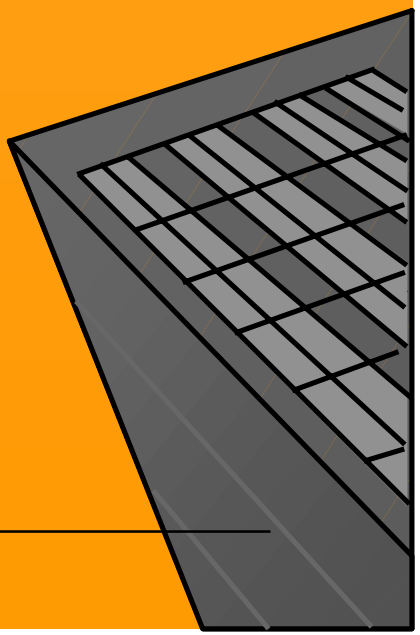


Enterprise Reality

New Orleans

May 3-6, 1998



Creating Data Confidence Through Access Controls and Electronic Signatures

Carol Mancuso

czm@inel.gov

Lockheed Martin Idaho Technologies Company

Idaho National Engineering and Environmental Laboratory

Prepared for the U.S. Department of Energy under DOE Idaho Operations Office contract DE-AC07-94ID13223.

Overview

- **Summary of the TRIPS application**
- **Critical business needs**
- **Security model**
- **Electronic signature applied to databases**

The Problem

- **Significant quantity of Nuclear Waste**
- **Governor's agreement with the Federal Government**
- **Recorded content questionable**
- **Stringent requirements on what can be shipped**

TRIPS

SITE PROJECT OFFICE

TRANSPORTATION

Unix Uniface

Oracle

DATA GENERATION

CERTIFICATION

RCRA CONTAINER MANAGEMENT

TRIPS Characteristics

- **Wide**
  - Large variety of information
  - Many subsystem interfaces
- **Shallow**
  - Relatively few records
- **Complex**
  - Data Acquisition
  - Work Flow Enhancement
  - Inventory Tracking
  - Compliance Monitoring

Critical Needs for Success

- **Ensure a high degree of trust in the data**
- **Provide secure environment for a geographically dispersed user group while minimizing client maintenance**
- **Enhance process throughput by reducing paper handling (including pen/ink signatures)**

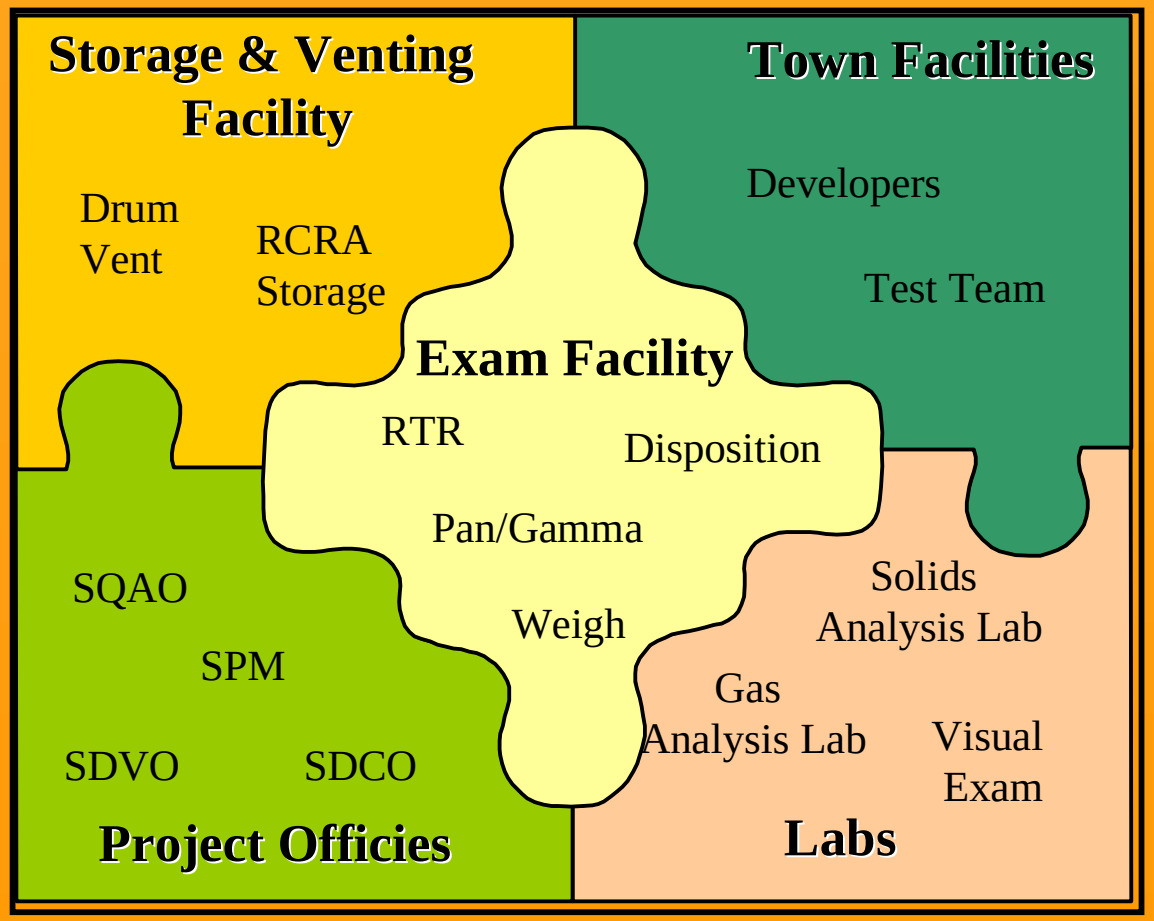
Solutions

- **Server centric architecture**
  - Security Model
  - Application Distribution
- **Electronic signature**

Security Model Requirements

- **Accommodate a geographically dispersed user group**
- **Minimize maintenance associated with client platforms**
- **Guarantee protection of the system**
- **Maintain flexibility in connecting to diverse data sources**

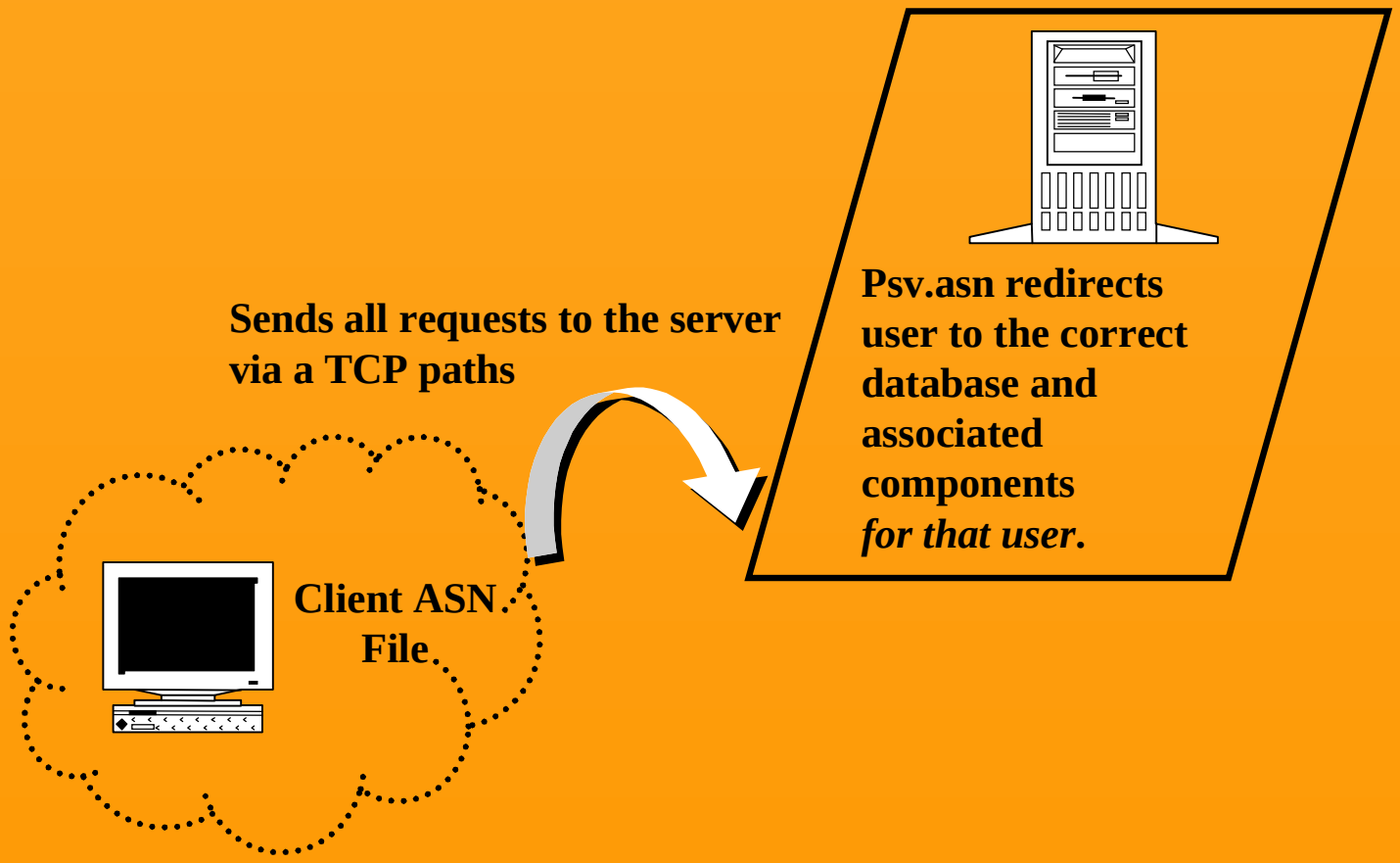
TRIPS User Community



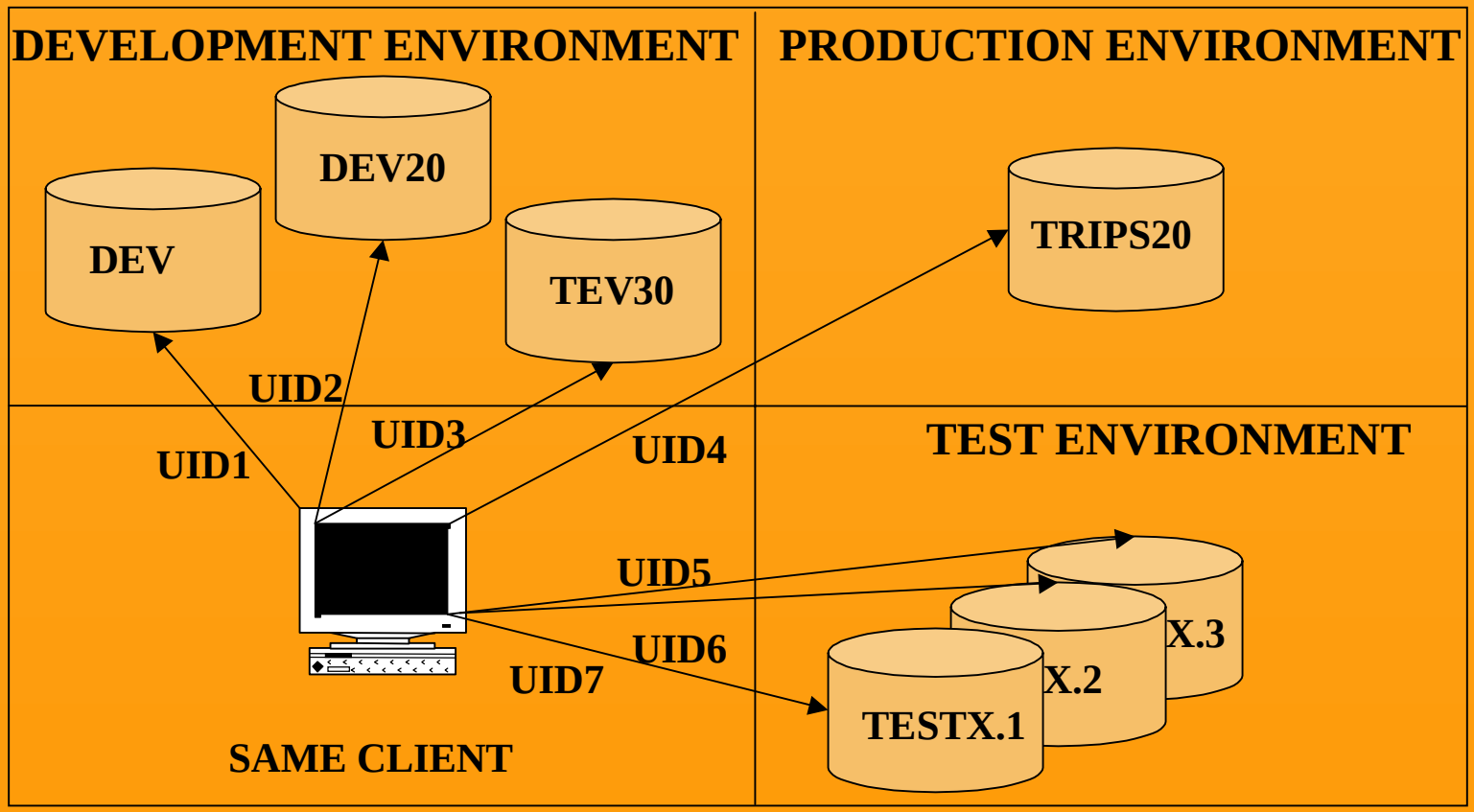
Approach for the Security Model

- **Minimize client dependence**
  - Client security not counted as part of the model
  - Centralized assignment file maintenance
  - Forms served from server via Polyserver
- **Guarantee system security**
  - Use Unix system authentication with restricted shells
  - Use Oracle role-based access controls
  - Use TRIPS role-based navigation restrictions

Smoke and Mirrors

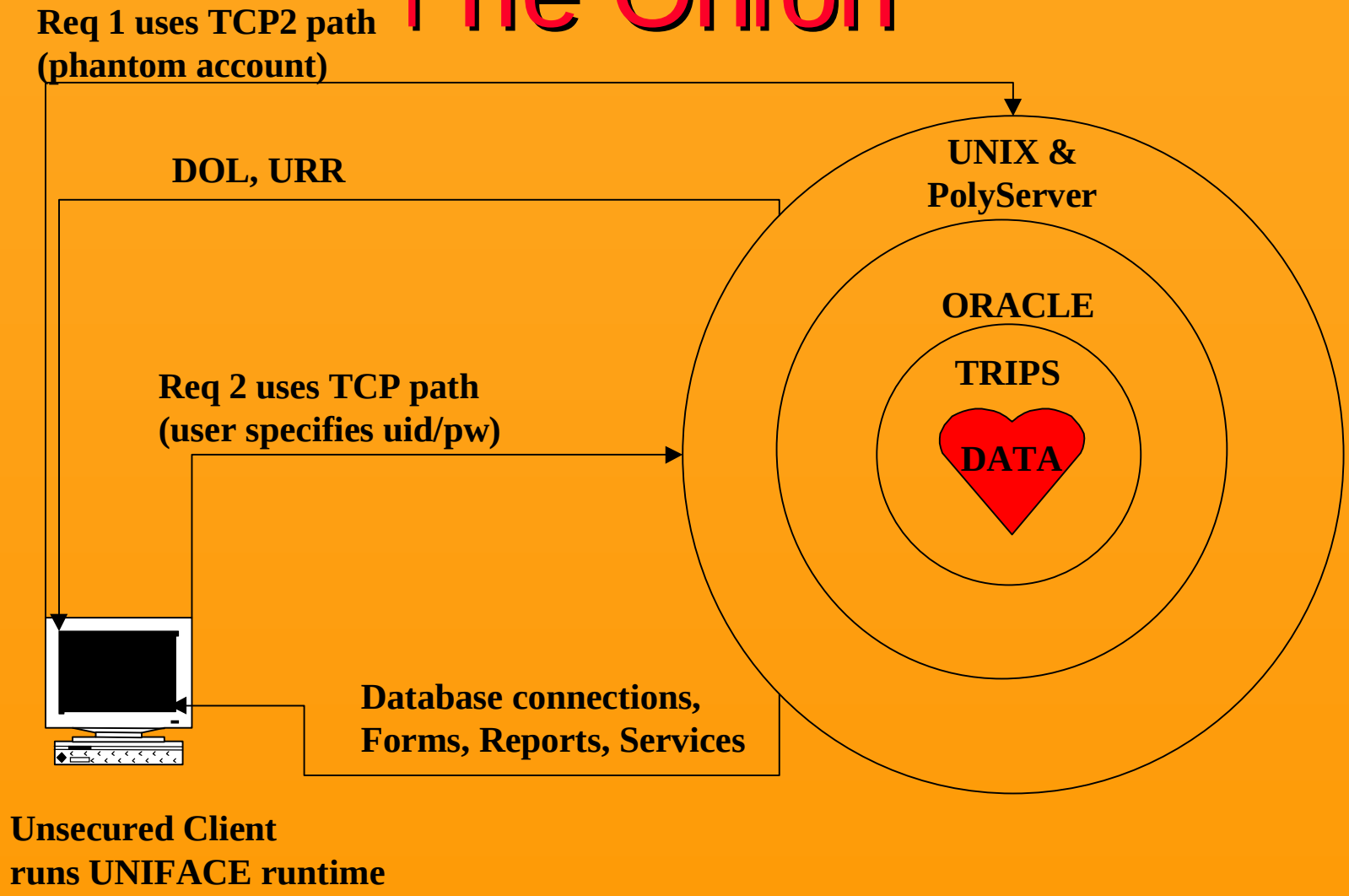


Useful Redirection



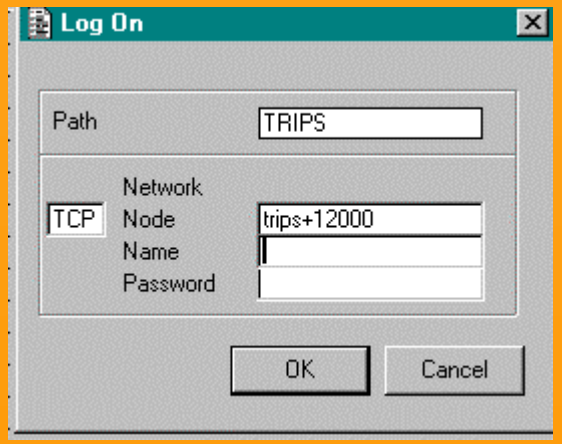
UID1 - UID 3 = member of the development team
UID4 = drum-vent operator
UID5 - UID7 = member of the test team

The Onion

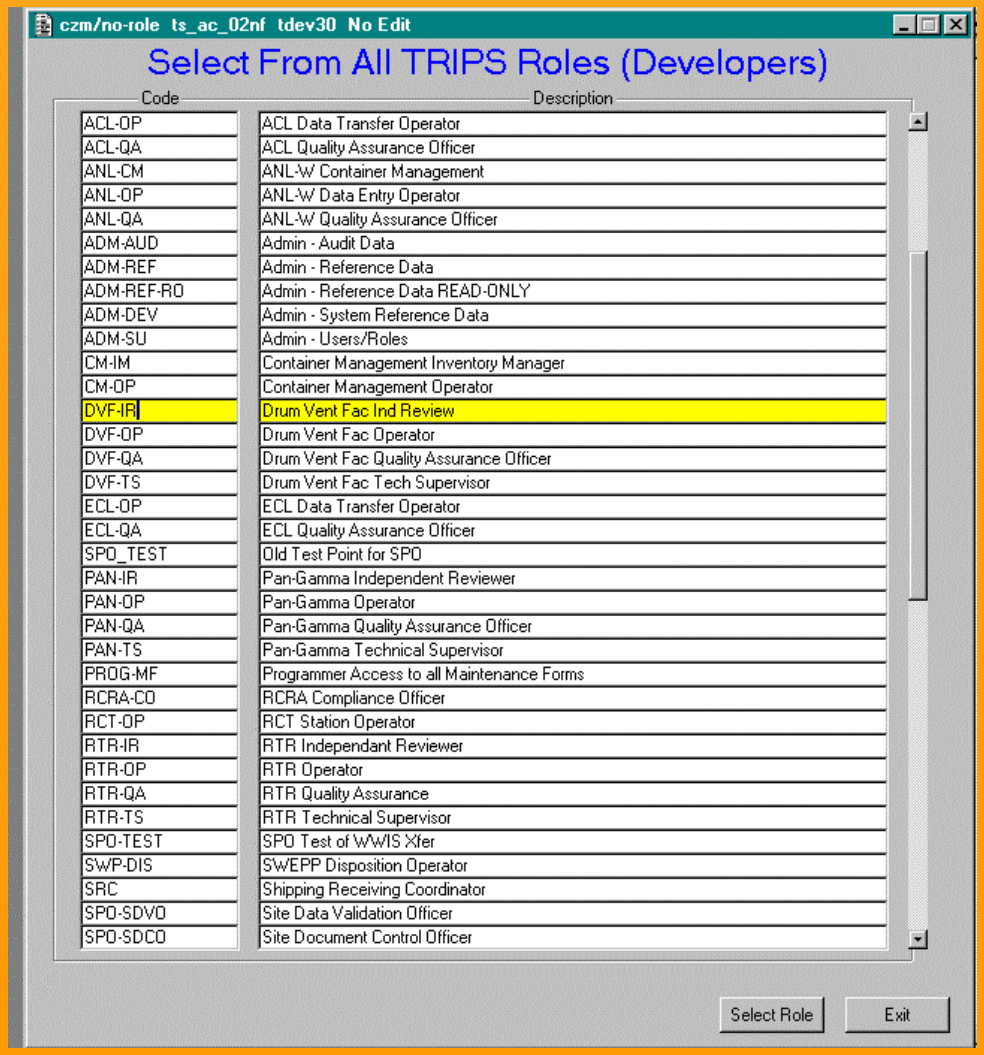


Unsecured Client
runs UNIFACE runtime

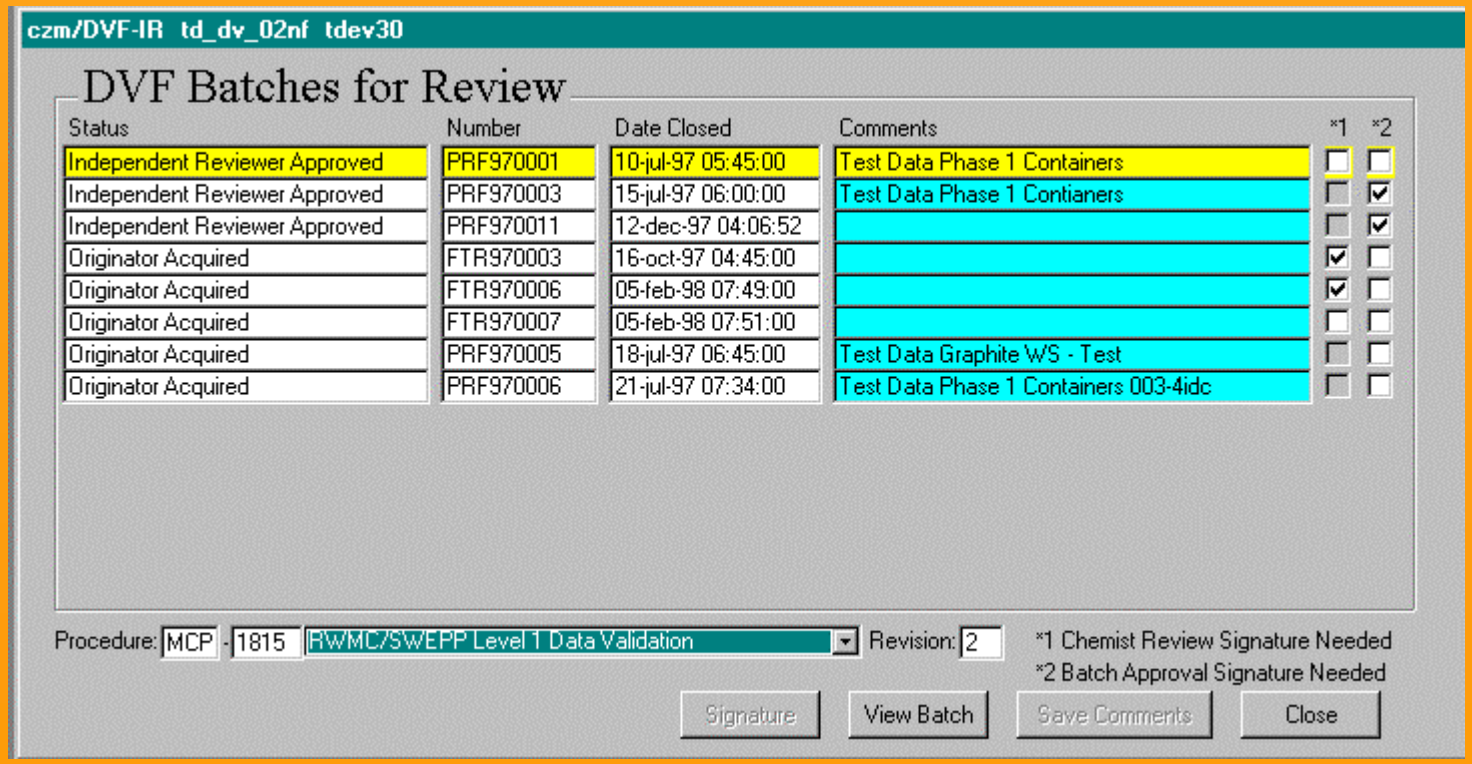
Log On


Log On
Path
TRIPS
Network
TCP
Node
trips+12000
Name
Password
OK
Cancel

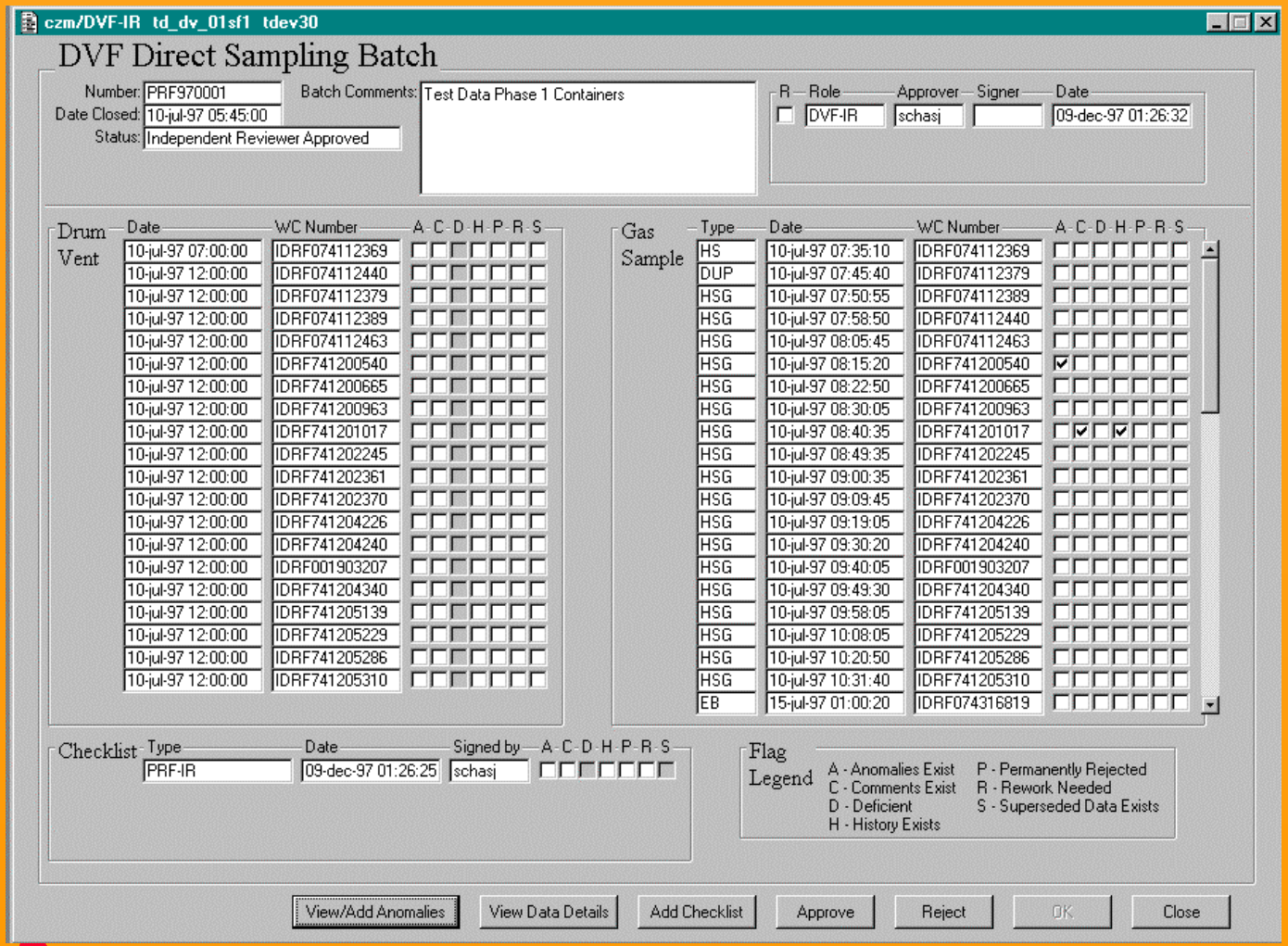
Role Selection



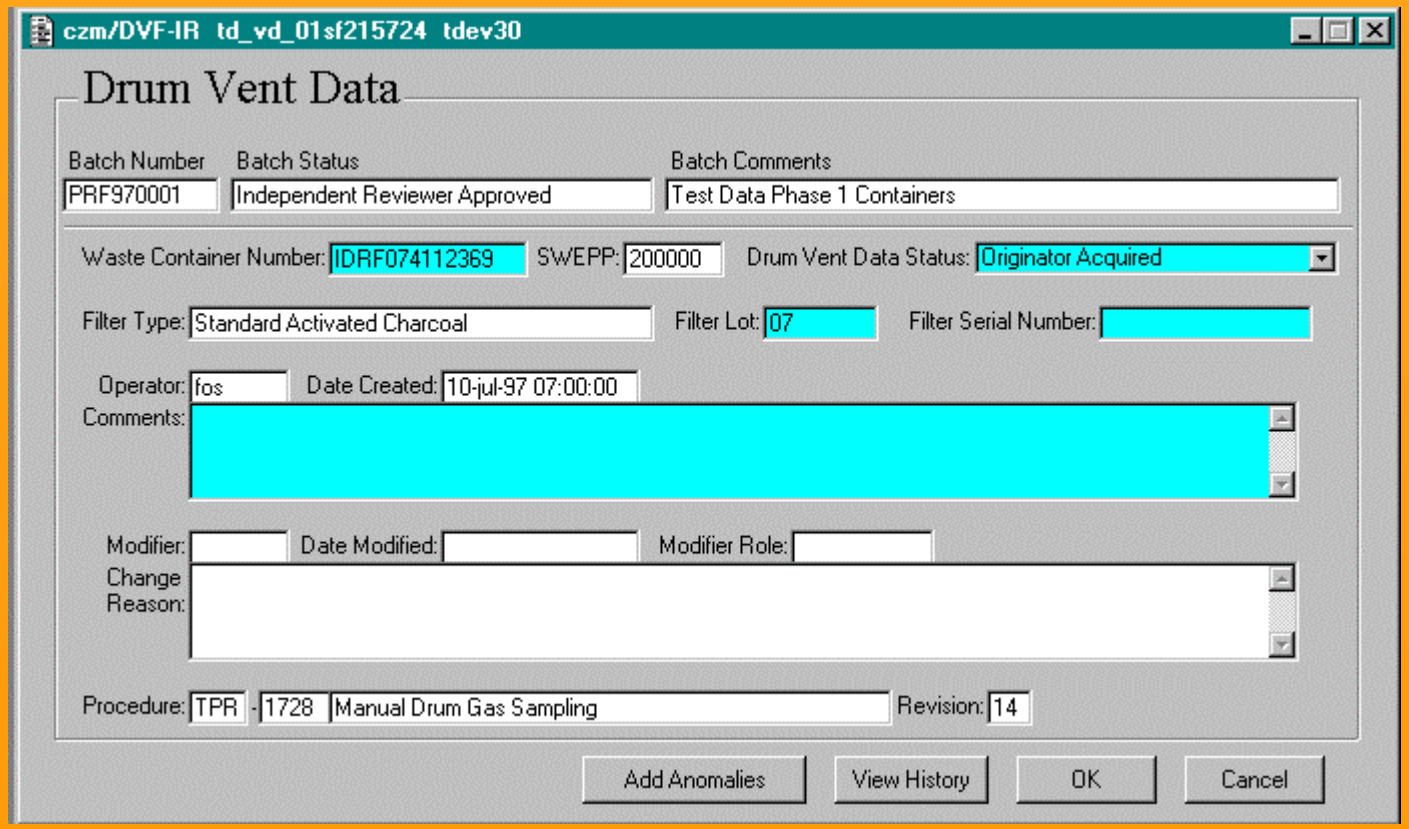
DVF-IR Role


czm/DVF-IR td_dv_02nf tdev30
DVF Batches for Review
Status
Number
Date Closed
Comments
*1
*2
Independent Reviewer Approved
PRF970001
10-jul-97 05:45:00
Test Data Phase 1 Containers
Independent Reviewer Approved
PRF970003
15-jul-97 06:00:00
Test Data Phase 1 Contianers
Independent Reviewer Approved
PRF970011
12-dec-97 04:06:52
Originator Acquired
FTR970003
16-oct-97 04:45:00
Originator Acquired
FTR970006
05-feb-98 07:49:00
Originator Acquired
FTR970007
05-feb-98 07:51:00
Originator Acquired
PRF970005
18-jul-97 06:45:00
Test Data Graphite WS - Test
Originator Acquired
PRF970006
21-jul-97 07:34:00
Test Data Phase 1 Containers 003-4idc
Procedure: MCP - 1815 RWMC/SWEPP Level 1 Data Validation
Revision: 2
*1 Chemist Review Signature Needed
*2 Batch Approval Signature Needed
Signature
View Batch
Save Comments
Close

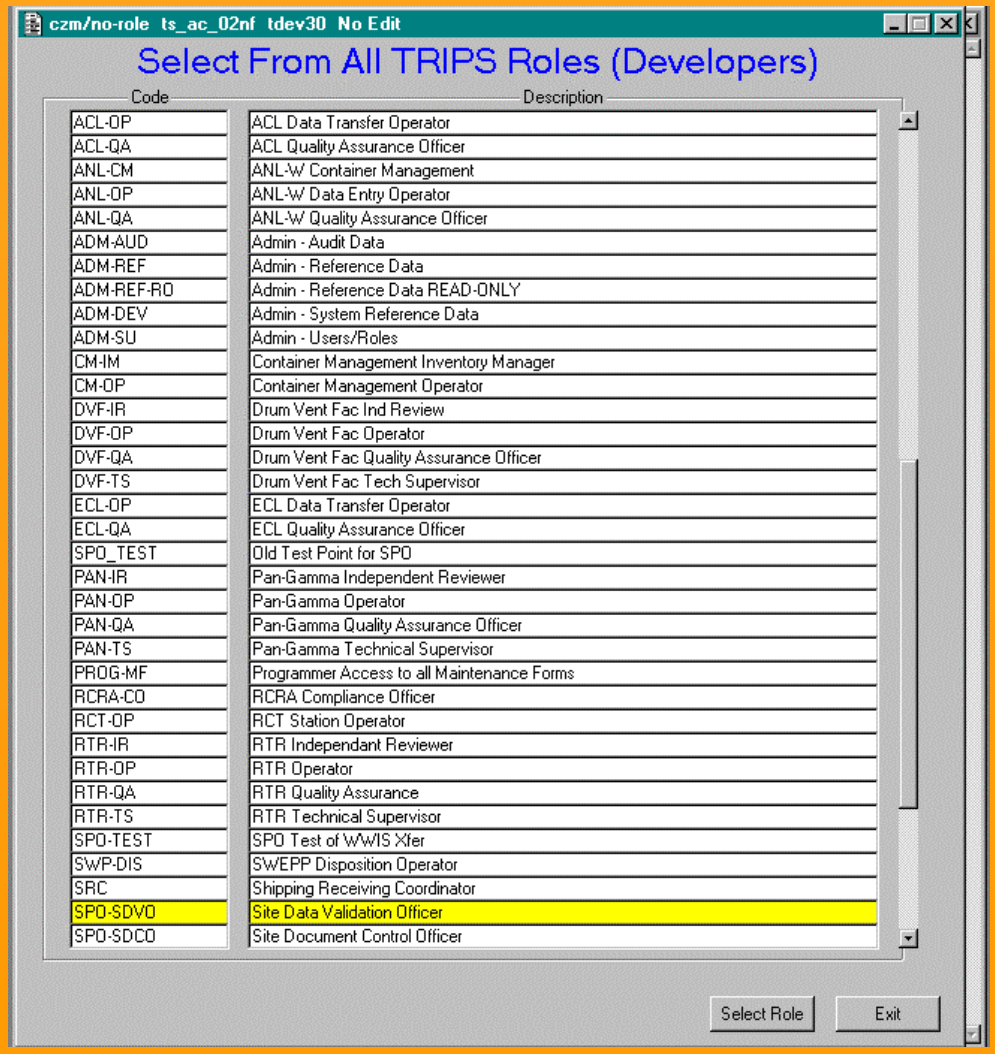
DVF-IR Role Cont.



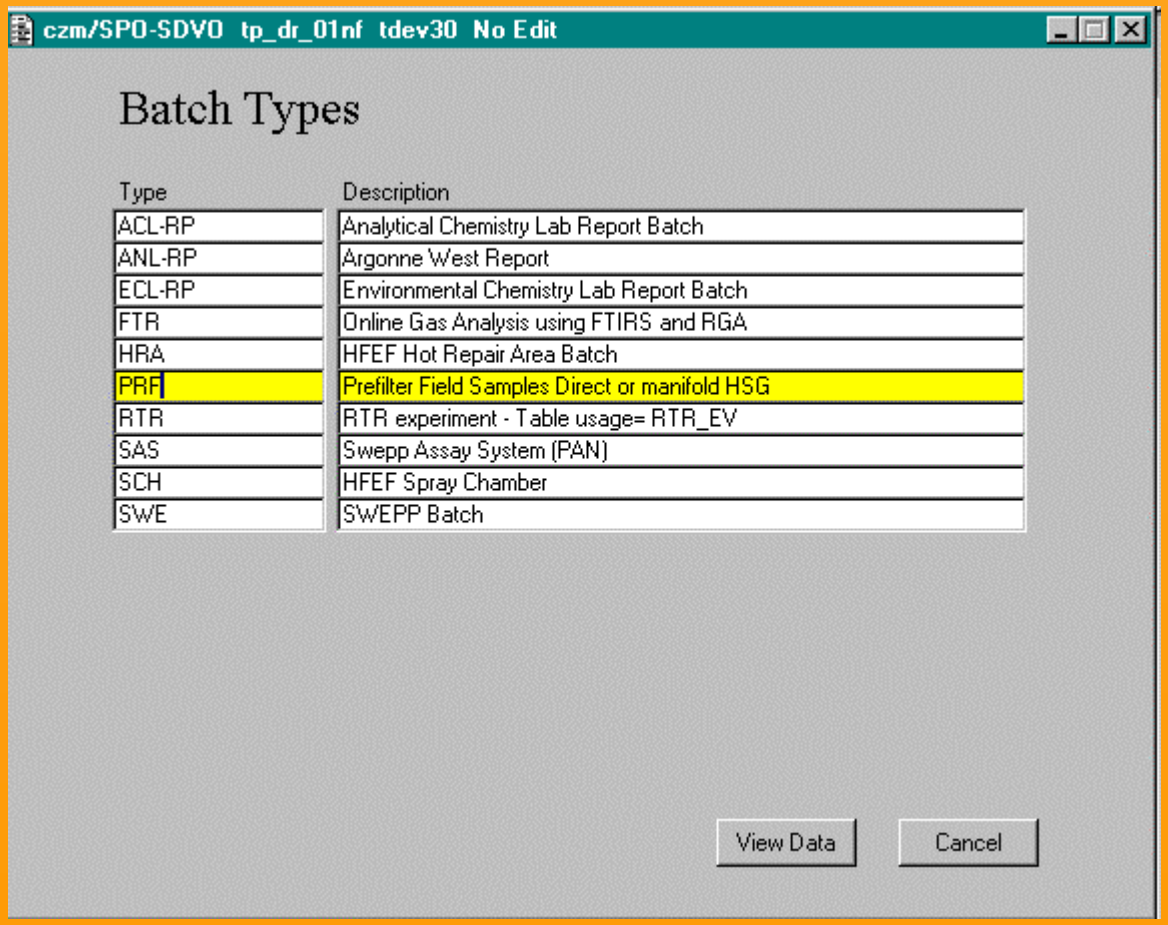
DVF-IR Role Cont.



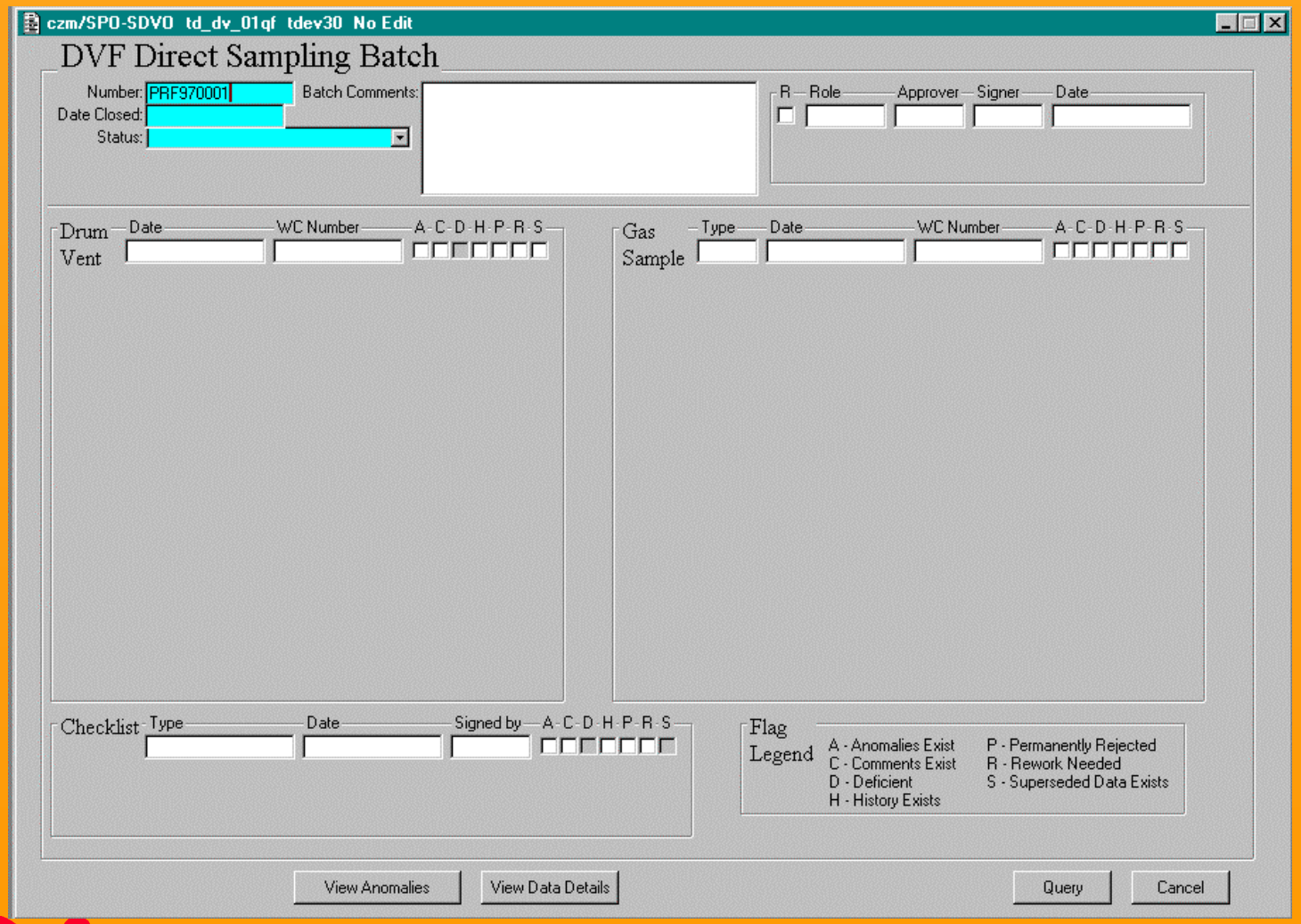
SPO-SDVO Role



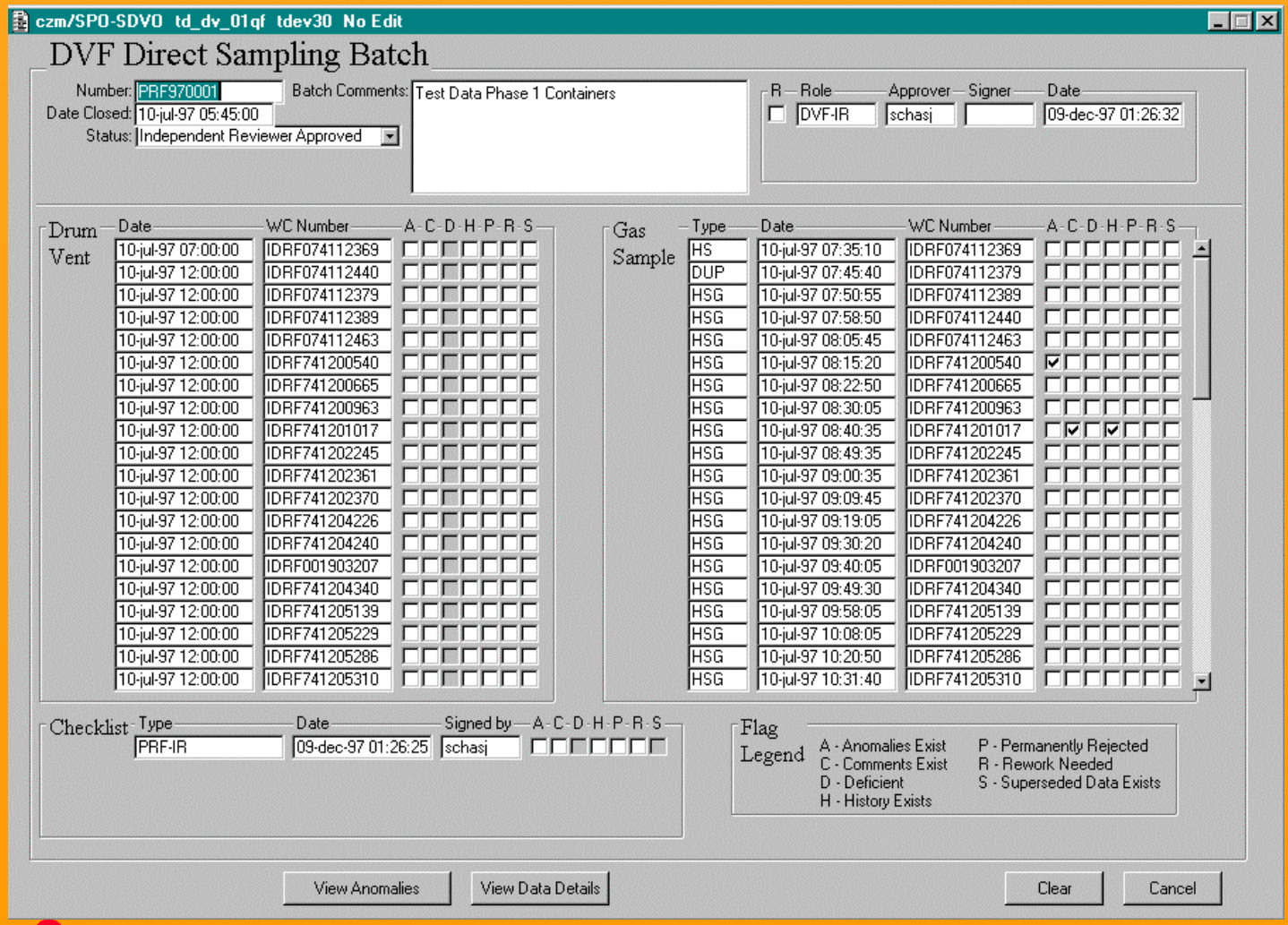
SPO-SDVO Role Cont.



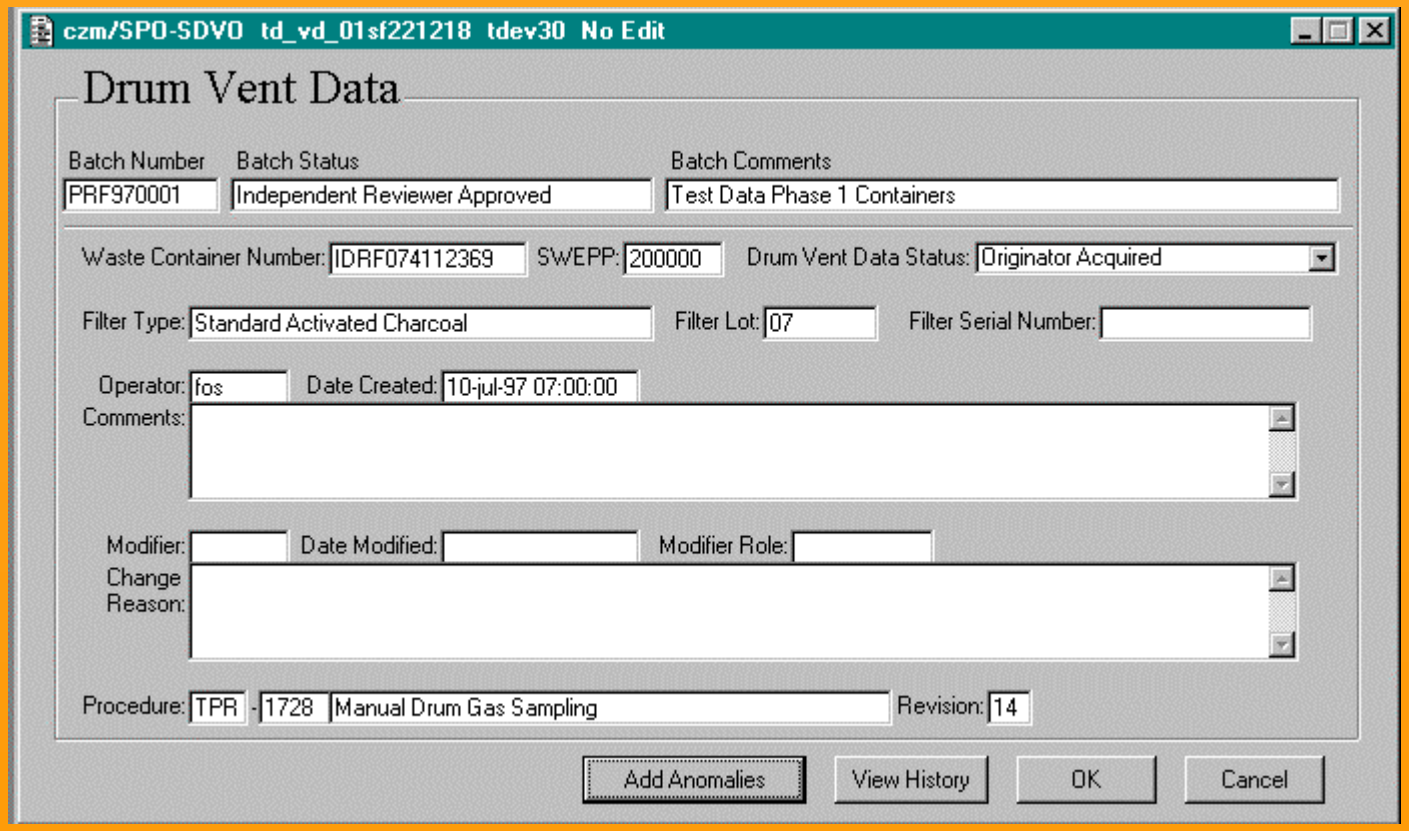
SPO-SDVO Role Cont.



SPO-SDVO Role Cont.



SPO-SDVO Role Cont.



Benefits

- **End users can't easily tamper with their configuration**
- **Distribution of new system versions is simplified**
- **Enhances ability to segregate development, test, and production environments**
- **Enhances ability to do effective CM**

Electronic Signature

- **What is it?**
- **TRIPS implementation of electronic signature**
- **TRIPS signature services**
- **TRIPS application of electronic signature to a database**
- **Benefits**

Electronic Signature Options

- **Shared secret data access control**
- **Digitization of handwritten signature**
- **Biometric Signature**
- **Public Key Cryptography (chosen method)**

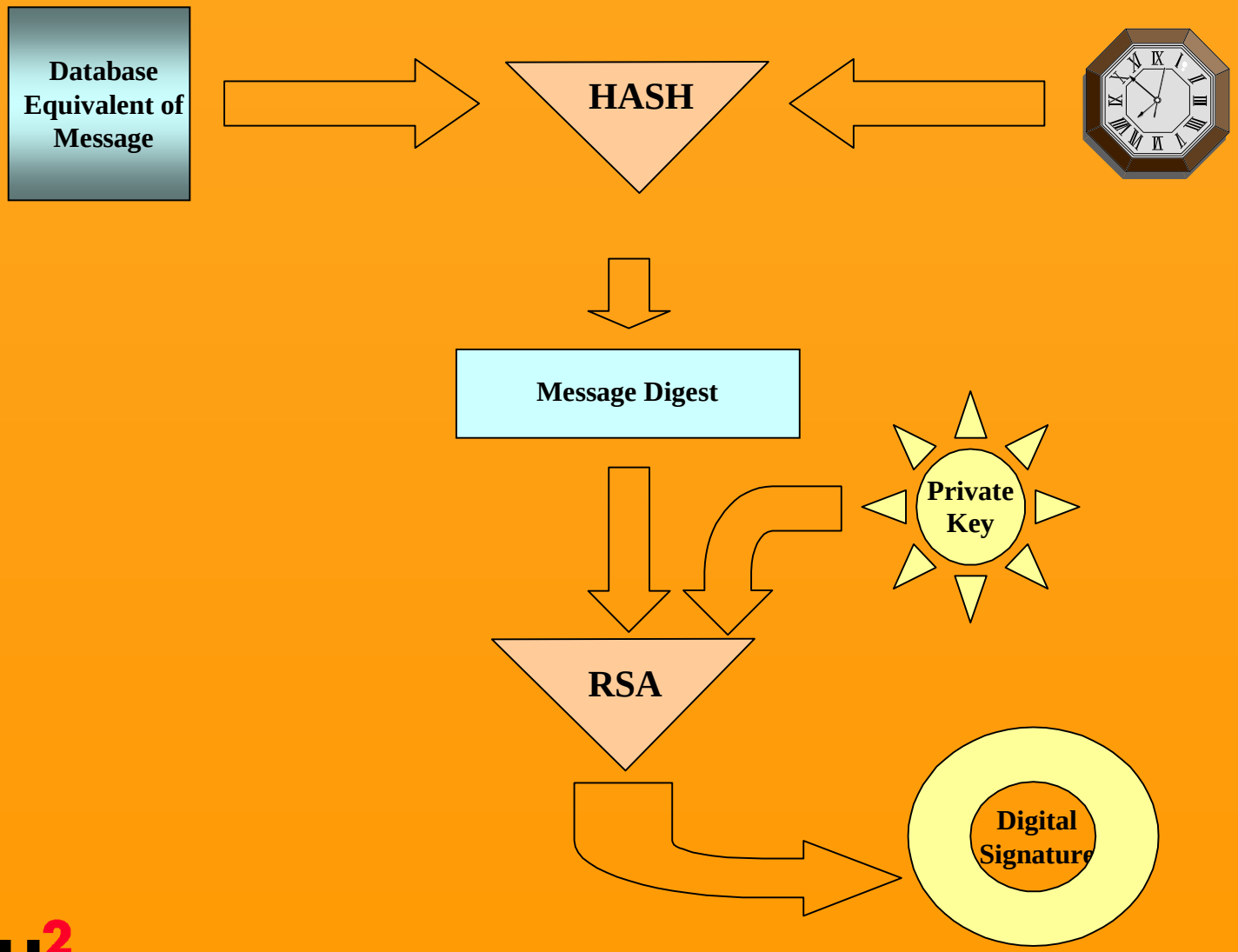
What is a Digital Signature?

- **Digital Signature is a unique set of bits which:**
  - represents the signers identity,
  - represents the data signed,
  - is non-reputable.

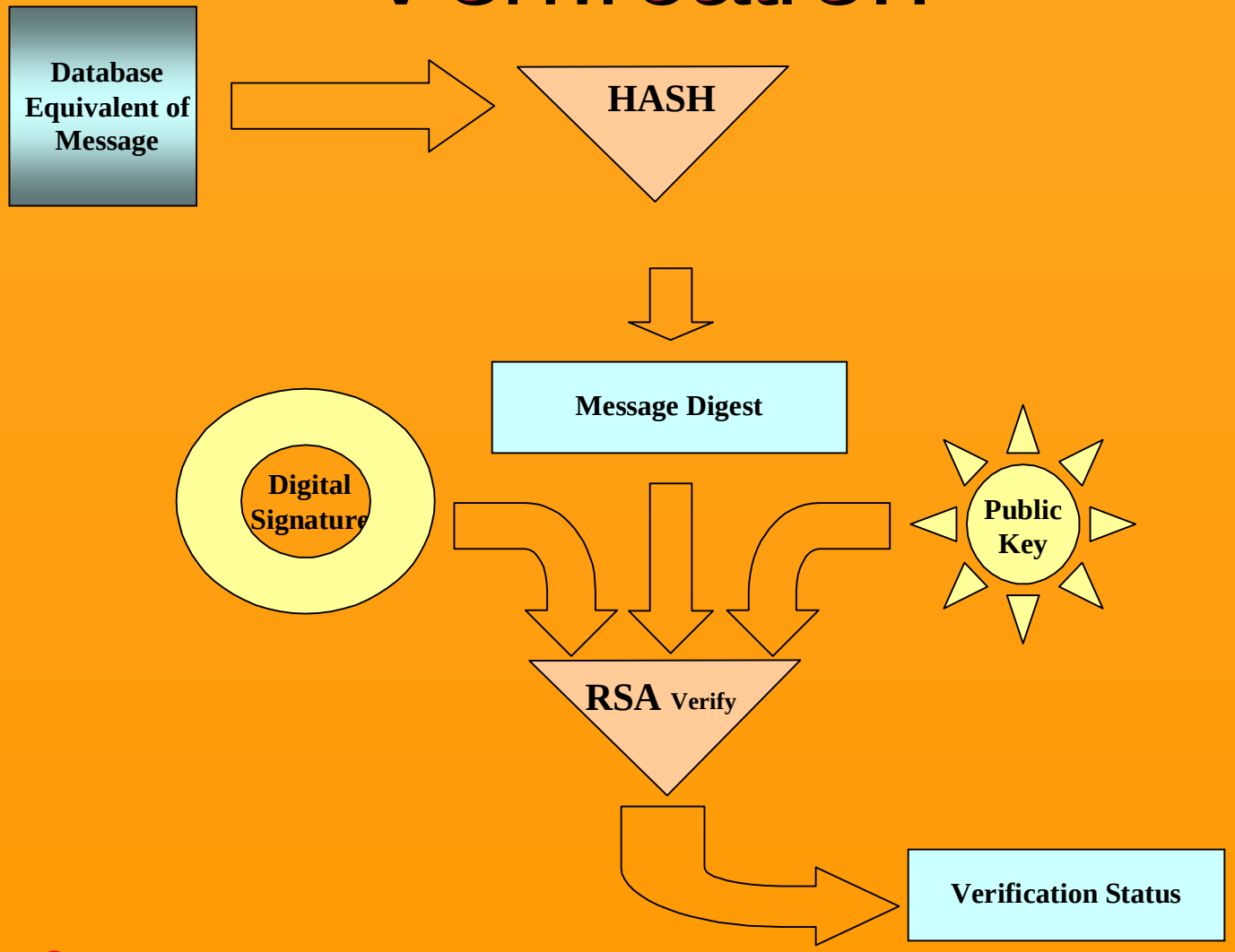
What is a Digital Signature?

- **Non-Reputable: Authenticity of *both* data and signer is not questionable.**
- **Public Key: Verifies signature and is certified and widely distributed.**
- **Private Key: Creates the signature and is held privately by the signer.**

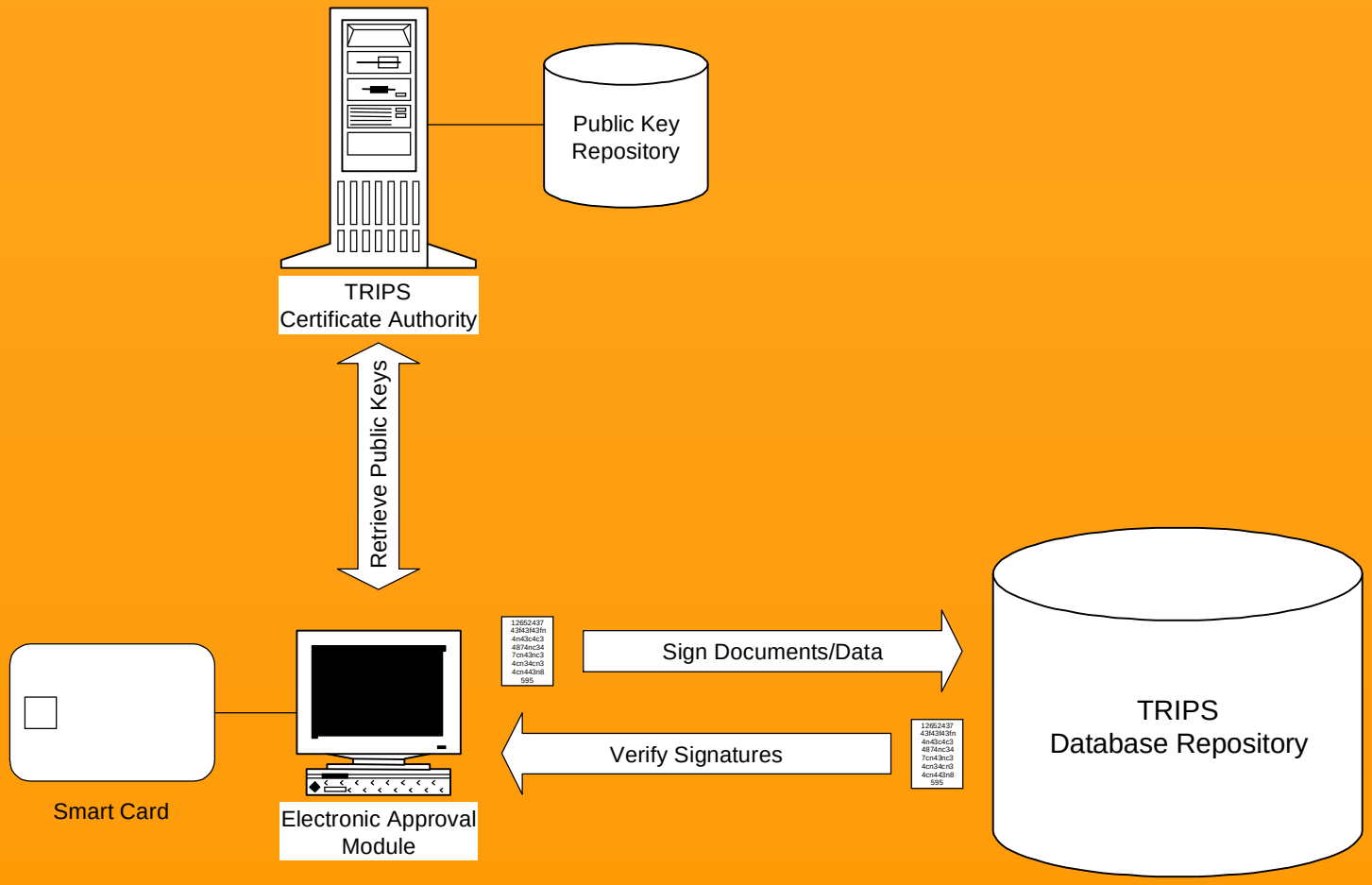
PKCS Signature Creation



PKCS Signature Verification



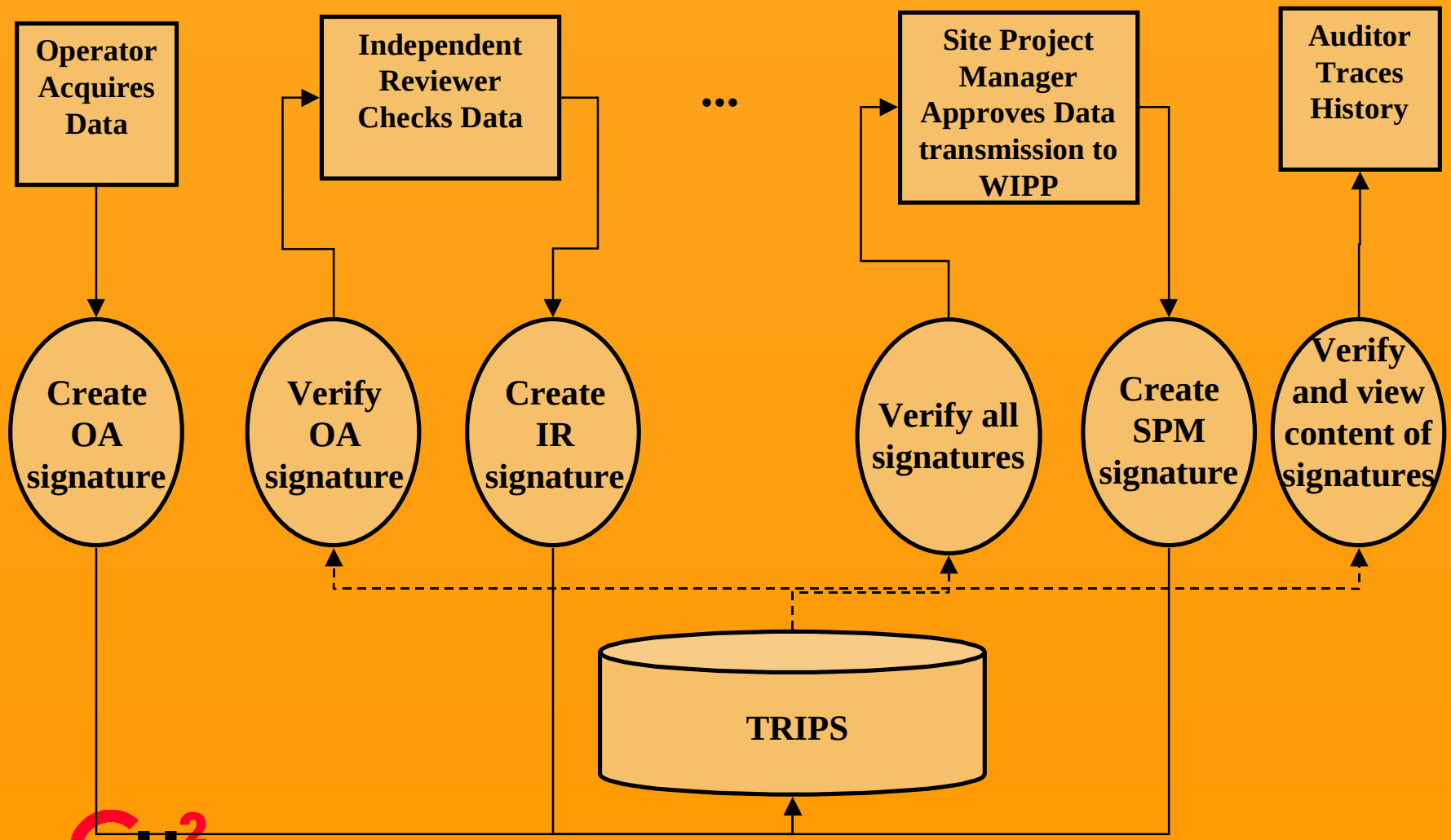
TRIPS Implementation



TRIPS Signature Services

- **Three signature types: approval set, batch, container set**
- **Two general types of services per signature type: sign, verify**
- **Implemented as hidden forms, *not* services (3GL interface required)**

Application of Electronic Signatures



Benefits

- **Eliminates paper**
- **Cost savings**
- **Legally binding**
- **In-process verification easier**
- **Tracking signatures becomes inherent**
- **Applicable to diverse applications**

CONTACTS

- **Business Contact**
  - Toni Austin, Manager, Advanced Computer Interface Products
    - (208) 526-3140
    - ama@inel.gov
- **Technical Contact**
  - Carol Mancuso, Project Level Subsystem Lead
    - (208) 526-2665
    - czm@inel.gov
- **Contributors**
  - Ben Groeneveld, Software Technical Lead
  - Wayne Austad, System Services Subsystem Lead
  - Stuart Walsh, Electronc Signature Subsystem Lead
  - Rich Oesterling, Configuration Management